AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1.-36. (Canceled)

37. (New) Apparatus for mediating in management orders between a plurality of origin managers and a plurality of managed devices in a telecommunications system, the management orders intended to execute management operations over the managed devices, comprising:

a communication receiver component arranged to receive a management order from an origin manager;

a management verifier component arranged to determine whether the received management order is an allowed management order by checking whether the management order fits an access attribute comprised in a management access template, the management access template being one selected from the group consisting of: a first management access template in relationship with an identifier of the origin manager; a second management access template in relationship with an identifier of a managed data object affected by the management order; and a third management access template in relationship with an identifier of a managed device affected by the management order; and

a communication sender component arranged to send an allowed management order to a managed device.

38. (New) The apparatus of claim 37, wherein the first management access template further comprises at least one access attribute selected from the group consisting of: an identifier of an allowed management operation; an identifier of an allowed managed data object; a pattern structure of the managed data object; an

identifier of an allowed managed device; an identifier of an allowed management operation over an allowed managed device; and an identifier of an allowed management operation over an allowed managed data object.

39. (New) The apparatus of claim 37, wherein the second management access template further comprises at least one access attribute selected from the group consisting of: a pattern structure of the managed data object; an identifier of an allowed management operation; an identifier of a managed device holding the managed data object; an identifier of an allowed origin manager; an identifier of an allowed management operation from an allowed origin manager; and an identifier of an allowed management operation over a holding managed device.

40. (New) The apparatus of claim 37, wherein the third management access template comprises at least one access attribute selected from the group consisting of: an identifier of an allowed management operation; an identifier of a managed data object held on the managed device; an identifier of an allowed origin manager; an identifier of an allowed management operation from an allowed origin manager; and an identifier of an allowed management operation over a held managed data object.

41. (New) The apparatus of claim 37, wherein the management verifier component is arranged to determine, from the identifier of a management operation, at least one identifier, the identifier being one selected from the group consisting of: an identifier of a managed data object affected by the operation; and an identifier of a managed device, affected by the operation.

42. (New) The apparatus of claim 37, wherein the management verifier component is arranged to select a management access template, among the first second and third management templates, according to an identifier received in a management order.

43. (New) The apparatus of claim 42, wherein the management verifier component is arranged to select a management access template, among the first second and third management templates, according to an access attribute comprised in another selected management access template.

44. (New) The apparatus of claim 42, wherein the identifier (ORID) of an origin manager comprises at least one identifier selected from the group consisting of: an identifier of a management server sending a management order; and an identifier of a user operating the management server; and

wherein the management verifier component is arranged to select the first management access template according to the at least one identifier.

45. (New) The apparatus of claim 42, wherein the identifier (ORID) of an origin manager comprises at least one identifier selected from the group consisting of: an identifier of a management server sending a management order; and an identifier of a user operating the management server; and wherein the management verifier component is arranged to authenticate the at least one identifier.

46. (New) The apparatus of claim 42, wherein the management verifier component is arranged to determine a management role associated to at least one identifier, the identifier being one selected from the group consisting of: an identifier of a management server sending a management order; and an identifier of a user operating the management server.

47. (New) The apparatus of claim 46, wherein the management verifier component is further arranged to select at least one management access template in relationship with the role.

48. (New) The apparatus of claim 46, wherein at least one management access template among the second or third management templates comprises an identifier (ROm) of at least one role as an access attribute, and wherein the

Management Verifier Component is further arranged to check whether the management order fits with the role.

49. (New) The apparatus of claim 37, wherein the management verifier component is arranged to determine whether a managed data object affected by an allowed management order is an access attribute in a management access template, and further comprising a management execution component, arranged to execute a management operation over the access attribute.

50. (New) The apparatus of claim 37, wherein the communication receiver component is further arranged to receive an access request from an origin manager;

wherein the management verifier component is further arranged to determine the first management access template; and

wherein the communication sender component is further arranged to send an access response to the origin manager that comprises an access attribute of the management access template.

51. (New) In a telecommunications system, a method for mediating in the management of a plurality of devices from a plurality of origin managers , comprising the steps of:

receiving a management order from an origin manager in the managed device;

executing a management operation requested by the management order in the managed device;

the step of receiving a management order comprising the further steps of:

receiving a management order in a centralized management mediator;

checking in the centralized management mediator whether the management order fits an access attribute comprised in a management access template so to determine whether a received management order is an allowed management order, the management access template being one selected from the group consisting of: a first management access template in relationship with an identifier of the origin manager; a second management access template in relationship with an identifier of a managed

data object affected by the management order; and a third management access template in relationship with an identifier of a managed device affected by the management order; and

granting the management order to be sent to a managed device if it is an allowed management order.

52. (New) The method of claim 51, wherein the step of checking the management order comprises the further step of determining, from the identifier of a management operation, at least one identifier selected from the group consisting of: an identifier of a managed data object affected by the operation; and an identifier of a managed device, affected by the operation.

53. (New) The method of claim 52, wherein the step of checking the management order comprises the further step of selecting a management access template, among the first second and third management templates, according to an identifier received in a management order.

54. (New) The method of claim 53, wherein the step of checking the management order comprises the further step of selecting a management access template, among the first second and third management templates, according to an access attribute comprised in another selected management access template.

55. (New) The method of claim 53, wherein the identifier (ORID) of an origin manager comprises at least one identifier among: an identifier of a management server sending a management order; an identifier of a user operating the management server; and

wherein the step of selecting a management access template comprises the further step of selecting the first management access template according to the at least one identifier.

56. (New) The method of claim 53, wherein the identifier (ORID) of an origin manager comprises at least one identifier selected from: an identifier of a management server sending a management order; and an identifier of a user operating the management server; and

wherein the step of checking the management order comprises the further step of authenticating the at least one identifier.

57. (New) The method of claim 53, wherein the step of checking the management order comprises the further step of determining a management role associated to at least one identifier selected from: an identifier of a management server sending a management order; and an identifier of a user operating the management server.

58. (New) The method of claim 57, wherein the step of checking the management order comprises the further step of selecting a management access template in relationship with the role.

59. (New) The method of claim 57, wherein at least one management access template among the second or third management templates comprises an identifier (ROm) of at least one role as an access attribute, and wherein the step of checking the management order comprises the further step of checking whether the management order fits with the role.

60. (New) The method of claim 51, wherein the step of checking the management order comprises the further step of checking whether a managed data object affected by an allowed management order is an access attribute in a management access template; and wherein the step of granting the management order comprises the further step of executing a management operation over the access attribute.

61. (New) The method of claim 51, comprising the further steps of:

receiving an access request from an origin manager;

determining the first management access template; and

sending an access response to the origin manager that comprises an access attribute of the management access template.

62. (New) A computer program for mediating from a computer-based apparatus in management orders between a plurality of origin managers and a plurality of managed devices in a telecommunications system, the management orders intended to execute management operations over the managed devices, comprising:

a computer-readable program having code adapted to cause a computer-based apparatus to process the reception of a management order from an origin manager;

the computer-readable program having code adapted to cause the computer-based apparatus to determine whether a received management order is an allowed management order by checking whether the management order fits an access attribute in a management access template, the management access template being one selected from the group consisting of: a first management access template in relationship with an identifier of the origin manager; a second management access template in relationship with an identifier of a managed data object affected by the management order; and a third management access template in relationship with an identifier of a managed device affected by the management order, and

the computer-readable program having code adapted to cause the computer-based apparatus to send an allowed management order to a managed device.

63. (New) The computer program of claim 62, further comprising the computer-readable program having code adapted to cause the computer-based apparatus to determine, from the identifier of a management operation, at least one identifier selected from: an identifier of a managed data object affected by the operation; and an identifier of a managed device, affected by the operation.

64. (New) The computer program of claim 62, further comprising the computer-readable program having code adapted to cause the computer-based

apparatus to select a management access template, among the first second and third management templates, according to an identifier received in a management order.

65. (New) The computer program of claim 64, further comprising the computer-readable program having code adapted to cause the computer-based apparatus to select a management access template, among the first second and third management templates, according to an access attribute comprised in another selected management access template.

66. (New) The computer program of claim 64, wherein the identifier (ORID) of an origin manager comprises at least one identifier among: an identifier of a management server sending a management order; an identifier of a user operating the management server; and

the computer-readable program having code adapted to cause the computer-based apparatus to select the first management access template according to the at least one identifier.

67. (New) The computer program of claim 64, wherein the identifier (ORID) of an origin manager further comprises at least one identifier selected from among: an identifier of a management server sending a management order; an identifier of a user operating the management server; and

wherein the computer-readable program has code adapted to cause the computer-based apparatus to authenticate the at least one identifier.

68. (New) The computer program of claim 64, further comprising the computer-readable program having code adapted to cause the computer-based apparatus to determine a management role associated to at least one identifier selected from: an identifier of a management server sending a management order; and an identifier of a user operating the management server.

69. (New) The computer program of claim 68, further comprising the computer-readable program having code adapted to cause the computer-based apparatus to select at least one management access template in relationship with the role.

70. (New) The computer program of claim 68, wherein at least one management access template among the second or third management templates comprises an identifier (ROm) of at least one role as an access attribute, and further comprising a computer-readable program code for causing the computer-based apparatus to check whether the management order fits with the role.

71. (New) The computer program of claim 62, further comprising the computer-readable program having code adapted to cause the computer-based apparatus to determine whether a managed data object affected by an allowed management order is an access attribute in a management access template, and a computer-readable program code for causing the computer-based apparatus to execute a management operation over the access attribute.

72. (New) The computer program of claim 62, further comprising:

the computer-readable program having code adapted to cause the computer-based apparatus to process the reception of an access request from an origin manager;

the computer-readable program having code adapted to cause the computer-based apparatus to determine the first management access template, and

the computer-readable program having code adapted to cause the computer-based apparatus to send an access response to the origin manager that comprises an access attribute of the management access template.